(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2002－278931
（P2002－278931A）
(43)公開日　平成14年９月27日(2002.9.27)

(51)Int.Cl.'		識別記号	FI		テーマコード'(参考)
Ｇ０６Ｆ	15/00	３３０	Ｇ０６Ｆ　15/00	３３０Ｂ	５Ｂ０１７
		３１０		３１０Ｄ	５Ｂ０８５
	12/14	３２０	12/14	３２０Ｆ	
	13/00	５１０	13/00	５１０Ｓ	
	17/60	３１４	17/60	３１４	

審査請求　有　請求項の数14　ＯＬ　（全９頁）

(21)出願番号　特願2001－81479(P2001－81479)

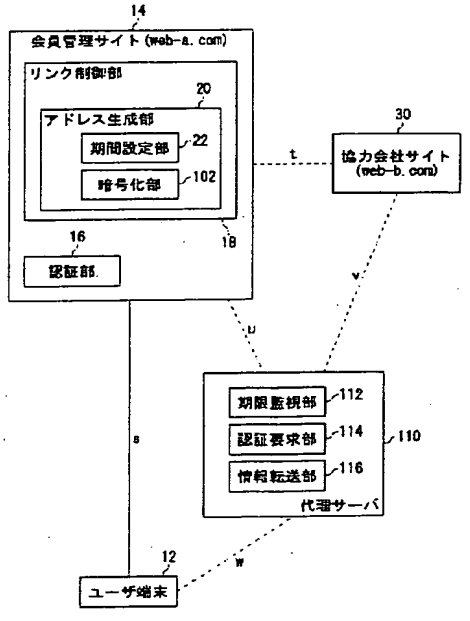
(22)出願日　平成13年３月21日(2001.3.21)

(71)出願人　397011373
ソニーコミュニケーションネットワーク株式会社
東京都品川区北品川４丁目７番35号
(72)発明者　森田　巧
東京都品川区北品川４丁目７番35号　ソニーコミュニケーションネットワーク株式会社内
(74)代理人　100105924
弁理士　森下　賢樹

Ｆターム(参考)　5B017 AA03 BA05 BA07 BB10
5B085 AA08 AE02 AE03 AE29 BA06
BC01

(54)【発明の名称】　ログイン管理方法およびシステム

(57)【要約】
【課題】　複数のサイトが協力関係をもっても、それぞれがユーザを認証すればユーザの利便性が悪く、サービスの一体感に欠ける。
【解決手段】　第１のサイトである会員管理サイト１４は、第２のサイトである協力会社サイト３０へのリンクを提供する。アドレス生成部２０は、ユーザがリンク個所をクリックしたとき代理サーバ１１０のＵＲＬをユーザ端末１２へ設定する。この際、サービスに時間制限を設ける。代理サーバ１１０は自ら協力会社サイト３０へログインし、情報をユーザ端末１２へ転送する。



1

【特許請求の範囲】

【請求項１】　ユーザが認証のための情報を入力してネットワーク上の第１のサイトへログインした後、そのサイトからリンクを辿って第２のサイトへのログインを試みたとき、第１のサイトにて前記認証のための情報を第２のサイトへアクセスするためのアドレスに付加して当該アクセスに提供することを特徴とするログイン管理方法。

【請求項２】　前記認証のための情報の有効期限を第１のサイトから第２のサイトへ適宜設定し、第２のサイトは第１のサイトからリンクを辿ってログインするユーザのアクセスを前記有効期限内に限り許可することを特徴とする請求項１に記載の方法。

【請求項３】　ユーザが所定のサイトへのログインを試みたとき、そのユーザをそのサイトを代理する中継拠点へ導く工程と、

その中継拠点にて得られた前記サイトの情報をその中継拠点からユーザへ提供する工程とを含み、

前記中継拠点が前記サイトの情報を得る際、そのサイトに認証のための情報を送信し、そのサイトからひとりのユーザとして認証された後、そのサイトへログインすることを特徴するログイン管理方法。

【請求項４】　ユーザが認証のための情報を入力してネットワーク上の第１のサイトへログインした後、そのサイトからリンクを辿って第２のサイトへのログインを試みたとき、そのユーザを第２のサイトの代理サーバへ導く工程と、

その代理サーバにて得られた第２のサイトの情報をその代理サーバからユーザへ提供する工程とを含み、

前記代理サーバが第２のサイトの情報を得る際、第２のサイトからひとりのユーザとして認証された後、第２のサイトへログインすることを特徴するログイン管理方法。

【請求項５】　前記ユーザが前記リンクを辿る際、第１のサイトはそのユーザが第２のサイトの情報を得ることができる有効期限に関する情報を前記代理サーバへアクセスするためのアドレスへ付加して当該アクセスへ提供することを特徴とする請求項４に記載の方法。

【請求項６】　前記有効期限に関する情報は暗号化されており、前記代理サーバはその情報を復号して解釈し、その有効期限が切れたときそのユーザに対する第２のサイトの情報の提供を停止することを特徴とする請求項５に記載の方法。

【請求項７】　第１のサイトを含むログイン管理システムであって、

前記第１のサイトは、ユーザが認証のための情報を入力してログインを求めたときユーザを認証する認証部と、ログインしたユーザに対して第２のサイトへのリンクを提供するリンク制御部とを含み、

前記リンク制御部は、前記認証のための情報を付加した

2

形で前記ユーザが第２のサイトへアクセスするためのアドレスを生成するアドレス生成部を含むことを特徴とするログイン管理システム。

【請求項８】　前記第１のサイトはさらに、前記認証のための情報の有効期限を第２のサイトへ適宜設定する期限設定部を含むことを特徴とする請求項７に記載のシステム。

【請求項９】　ユーザが所定のサイトへアクセスする際、そのアクセスを仲介する中継拠点を含むログイン管理システムであって、

前記中継拠点は、

前記サイトから、自身がユーザとして認証を受けるために必要な情報を送信する認証要求部と、

前記サイトからユーザとして認証されたとき、このサイトへログインして取得した情報を前記ユーザへ提供する情報転送部と、

を含むことを特徴するログイン管理システム。

【請求項１０】　第１のサイトと代理サーバとを含むログイン管理システムであって、

前記第１のサイトは、ユーザが認証のための情報を入力してログインを求めたときユーザを認証する認証部と、ログインしたユーザに対して第２のサイトへのリンクを提供するリンク制御部とを含み、

前記リンク制御部は、前記ユーザが前記代理サーバへアクセスするためのアドレスを生成するアドレス生成部を含み、

前記代理サーバは、第２のサイトから、自身がユーザとして認証を受けるために必要な情報を送信する認証要求部と、第２のサイトからユーザとして認証されたとき、このサイトへログインして取得した情報を前記ユーザへ提供する情報転送部とを含むことを特徴するログイン管理システム。

【請求項１１】　前記アドレス生成部は、前記ユーザが第２のサイトの情報を得ることができる有効期限に関する情報を前記アドレスへ付加することを特徴とする請求項１０に記載のシステム。

【請求項１２】　前記アドレス生成部は、前記有効期限に関する情報を暗号化したうえで前記アドレスへ付加することを特徴とする請求項１１に記載のシステム。

【請求項１３】　前記代理サーバはさらに、前記有効期限に関する情報を解釈してその期限の経過を監視する期限監視部を含み、その期限が経過したとき前記ユーザへの情報の提供が停止されることを特徴とする請求項１１、１２のいずれかに記載のシステム。

【請求項１４】　ユーザが最初にログインする第１のサイトと代理サーバとを含むログイン管理システムであって、

前記代理サーバは前記第１のサイトと類似するドメイン名のもとで構築され、

ユーザが第１のサイトとセッションを有している間に第

２のサイトへのログインを要求したとき、前記第１のサイトはそのユーザのアクセス先を前記代理サーバへ変更し、

前記代理サーバは、そのユーザに代わって第２のサイトから情報を取得してこれをそのユーザへ提供することを特徴とするログイン管理システム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】この発明は、ログイン管理技術に関し、とくに、ユーザがネットワーク上のあるサイトへログインするとき、これを制御するログイン管理方法およびシステムに関する。

【０００２】

【従来の技術】ネットワーク、とくにインターネットを利用した電子商取引は、近い将来国家経済の大きな割合を占める勢いである。いわゆるＩＴ関連企業は当然としても、従来ＩＴとは無縁だった企業も、ウェブサイトを構築して情報を発信する姿勢が生き残りのための必要条件に思える状況である。

【０００３】こうした状況下、ＡＳＰ（Application Service Provider）ビジネスが拡大している。企業は最適なウェブサイトの設計、構築、および運用の一部または全部をＡＳＰに委託し、インターネットを通じたビジネスの拡張をアウトソーシングによって迅速かつ効率的に展開しつつ、既存ビジネスの安定確保に注力している。一方、インターネットを利用したビジネスの連携も急速に拡大している。たとえば、同業のメーカーが集合して部品調達の安定とコストダウンを図ったり、電子モールを形成してユーザによる選択の可能性を広げたりといった展開のほか、同一ブランドを利用する異業種連合も増えている。そうした場合、ＡＳＰには、それら同業または異業種の連合体がユーザから見たとき一体感をもつサービス設計が求められる。

【０００４】

【発明が解決しようとする課題】しかしながら実際には、企業毎にサイトのドメイン名が異なり、連合体としての一体感をウェブ上に形成することに壁がある。本発明はこの点を認識した本発明者によってなされたものであり、ひとつの目的は、複数主体の連携に一体感をもたせたサービスをログインの管理という技術要素から実現することにある。本発明の別の目的は、ビジネスが拡大しつつあるＡＳＰの観点から、一体感のあるサービスを実現することにある。本発明のさらに別の目的は、ユーザを会員として扱うサービスにおいて、ユーザのログインを簡略化しつつセキュリティ面にも考慮した技術を提供することにある。

【０００５】

【課題を解決するための手段】本発明のある態様は、ログイン管理方法に関する。この方法は、ユーザが認証のための情報を入力してネットワーク上の第１のサイトへ

ログインした後、そのサイトからリンクを辿って第２のサイトへのログインを試みたとき、第１のサイトにて前記認証のための情報を第２のサイトへアクセスするためのアドレスに付加して当該アクセスに提供するものである。

【０００６】ここで「サイト」は、サイト内のサーバその他任意のノードでよく、ここでは総称的にサイトと呼ぶに過ぎない。アドレスの例はＵＲＬ（Uniform Resource Locator）であり、例えばユーザが第１のサイトをウェブブラウザで閲覧しているとき、ページ上に設けられた第２のサイトへのリンクをクリックしたとする。このとき、ユーザのブラウザには第２のサイトのＵＲＬが設定される。本態様では、そのＵＲＬに認証のための情報（以下、単に認証情報ともよぶ）が付加される。例えばブラウザの機能によって認証情報とＵＲＬ本体が分解され、第２のサイトへアクセスするとともに、第２のサイトから発せられる認証の要求に自動対応することができる。認証情報の例としてユーザＩＤとパスワードの組があるが、もちろんこれに限られない。認証情報はそのままの形でアドレスに付加される場合のほか、ワンタイム化され、または暗号化された後に付加されてもよく、そうした場合も含めて「第１のサイトにて前記認証のための情報を第２のサイトへアクセスするためのアドレスに付加して当該アクセスに提供する」と表現する。

【０００７】この態様によれば、ユーザは第２のサイトへのログインの際に新たな認証手続を経る必要がない。したがって、例えば第１のサイトと第２のサイトが協力関係にある場合、ユーザの利便性を高め、かつサービスの一体感を醸成することができる。

【０００８】認証情報の有効期限を第１のサイトから第２のサイトへ適宜設定し、第２のサイトは第１のサイトからリンクを辿ってログインするユーザのアクセスを前記有効期限内に限り許可してもよい。「第１のサイトから第２のサイトへ」とは、必ずしも第１のサイトが主体的である必要はなく、第２のサイトがいわゆるプル型の動作で設定内容を取得してもよい。この設定は、例えばアクセスを許すユーザの認証情報を列記したリストで通知されてもよく、その場合、そのリストに記載する認証情報を適宜変更して通知することにより、実用上まったく問題なく有効期限を設定することができる。例えば、３０分間隔でリストを送信し、かつ、あるユーザの認証情報は１回に限りリストに載るようにすれば、事実上そのユーザの有効期限が３０分となる。ユーザごとにリストに載せる回数を変えれば、有効期限を変化させることもできる。なお当然ながら、ユーザの認証情報ごとに直接的に有効期限を記述して送信してもよい。

【０００９】本発明の別の態様もログイン管理方法に関する。この方法は、ユーザが所定のサイトへのログインを試みたとき、そのユーザをそのサイトを代理する中継拠点へ導く工程と、その中継拠点にて得られたサイトの

情報をその中継拠点からユーザへ提供する工程とを含む。この構成にて、中継拠点がサイトの情報を得る際、そのサイトに認証のための情報を送信し、そのサイトからひとりのユーザとして認証された後、そのサイトへログインする。

【００１０】本発明のさらに別の態様もログイン管理方法に関する。この方法は、ユーザが認証のための情報を入力してネットワーク上の第１のサイトへログインした後、そのサイトからリンクを辿って第２のサイトへのログインを試みたとき、そのユーザを第２のサイトの代理サーバへ導く工程と、その代理サーバにて得られた第２のサイトの情報をその代理サーバからユーザへ提供する工程とを含む。この構成において、代理サーバが第２のサイトの情報を得る際、第２のサイトからひとりのユーザとして認証された後、第２のサイトへログインする。

【００１１】この態様であれば、代理サーバがユーザに代わって第２のサイトへログインするため、ユーザ自身は再度ログインのための手続をとる必要がない。一方、そのユーザは第１のサイトへのログインの際には認証されているため、セキュリティ面でのケアはなされている。

【００１２】そのユーザがリンクを辿る際、第１のサイトはそのユーザが第２のサイトの情報を得ることができる有効期限に関する情報を代理サーバへアクセスするためのアドレスへ付加して当該アクセスへ供してもよい。また、有効期限に関する情報は暗号化されており、代理サーバはその情報を復号して解釈し、有効期限が切れたときそのユーザに対する第２のサイトの情報の提供を停止してもよい。

【００１３】有効期限を設ける利点はセキュリティにある。上述の構成の場合、第２のサイトはユーザの認証を第１のサイトへ委任することができる。あるユーザが第１のサイトへログインしたときに限り第２のサイトへのリンクが見える構成とすれば、第２のサイトへのアクセスを事実上制限できる。しかし、このユーザが第２のサイトへアクセスしている間にこれをブックマークした場合、以降このユーザでない者であっても、このブックマークを頼りに第２のサイトへアクセスしうる。いま、第２のサイトが会員のみに開示されるべき情報を発信していれば、セキュリティ面で改善の余地がある。このため、有効期限を比較的短く設定すれば、たとえブックマークされても、このユーザ以外の者による第２のサイトの閲覧を阻止しやすくなる。

【００１４】本発明のさらに別の態様は、ログイン管理システムに関する。このシステムは、第１のサイトを含む。第１のサイトは、ユーザが認証のための情報を入力してログインを求めたときユーザを認証する認証部と、ログインしたユーザに対して第２のサイトへのリンクを提供するリンク制御部とを含む。リンク制御部は、前記認証のための情報を付加した形で前記ユーザが第２のサイトへアクセスするためのアドレスを生成するアドレス生成部を含む。

【００１５】本発明のさらに別の態様もログイン管理システムに関する。このシステムは、ユーザが所定のサイトへアクセスする際、そのアクセスを仲介する中継拠点を含む。この中継拠点は、前記サイトから、自身がユーザとして認証を受けるために必要な情報を送信する認証要求部と、前記サイトからユーザとして認証されたとき、このサイトへログインして取得した情報を前記ユーザへ提供する情報転送部とを含む。

【００１６】本発明のさらに別の態様もログイン管理システムに関する。このシステムは、第１のサイトと代理サーバとを含む。第１のサイトは、ユーザが認証のための情報を入力してログインを求めたときユーザを認証する認証部と、ログインしたユーザに対して第２のサイトへのリンクを提供するリンク制御部とを含む。リンク制御部は、前記ユーザが前記代理サーバへアクセスするためのアドレスを生成するアドレス生成部を含む。また、代理サーバは、第２のサイトから、自身がユーザとして認証を受けるために必要な情報を送信する認証要求部と、第２のサイトからユーザとして認証されたとき、このサイトへログインして取得した情報を前記ユーザへ提供する情報転送部とを含む。

【００１７】したがって、ユーザが第１のサイトへ認証を経てログインした後、第２のサイトへリンクを辿ってアクセスしようとしたとき、代理サーバへ接続される。代理サーバ自身はひとりのユーザとして第２のサイトから認証され、以降、そのサイトの情報をユーザへ提供する。

【００１８】代理サーバはさらに、有効期限に関する情報を解釈してその期限の経過を監視する期限監視部を含み、その期限が経過したとき前記ユーザへの情報の提供が停止されてもよい。情報の提供の停止は、代理サーバがそのユーザのために第２のサイトと張ったセッションを切断してもよいし、情報転送部による転送を禁止してもよい。

【００１９】本発明のさらに別の態様もログイン管理システムに関する。このシステムは、ユーザが最初にログインする第１のサイトと代理サーバとを含む。代理サーバは前記第１のサイトと類似のドメイン名のもとで構築される。類似は同一を含み、また第１のサイトのドメイン名のサブドメイン名などを含む。ユーザが第１のサイトとセッションを有する間に第２のサイトへのログインを要求したとき、第１のサイトはそのユーザのアクセス先を代理サーバへ変更する。代理サーバは、そのユーザに代わって第２のサイトから情報を取得してこれをそのユーザへ提供する。

【００２０】なお、以上の構成要素の任意の組合せや組み替え、本発明を方法、システム、コンピュータプログラム、記録媒体などと表現したものもまた、本発明の態

様として有効である。

【００２１】

【発明の実施の形態】実施の形態１．図１は、実施の形態１に係るログイン管理システム１０の構成を示す。ログイン管理システム１０において、ユーザ端末１２、第１のサイトである会員管理サイト１４、および第２のサイトである協力会社サイト３０が明示しないインターネットで接続されている。会員管理サイト１４のドメイン名はweb-a.com、協力会社サイト３０のドメイン名はweb-b.comである。

【００２２】会員管理サイト１４は、あるサービスに関して協力会社サイト３０と協力しており、そのサービスに関して会員を募集し、また会員に窓口として機能する。したがって、ログイン管理システム１０には協力会社サイト３０以外にも多数の協力会社が存在してもよく、その場合、窓口としての会員管理サイト１４の意義が高まる。一例として、会員管理サイト１４は会員に稀少商品を提供するバーチャルモールで、協力会社サイト３０はそれに出店している輸入雑貨店である。会員には会費をもらう関係上、協力会社サイト３０は会員のみにアクセスを認める。

【００２３】会員管理サイト１４は認証部１６、リンク制御部１８、および期限設定部２２を有する。認証部１６はユーザがログインを要求したとき（図中経路ｓ）、これを認証する。ユーザがこのサービスの会員になると、ユーザＩＤとパスワード（以下、認証情報ともいう）が与えられる。なお、以下とくに断らない限り、「ユーザ」と「会員」を表現上区別しない。

【００２４】認証されたユーザは会員管理サイト１４の会員用ページへログインできる。このページには種々の情報があり、その中に協力会社サイト３０へのリンクもある。このリンクは会員管理サイト１４にログインできたユーザのみに見えるようページが構成されている。

【００２５】リンク制御部１８はユーザがそのリンク個所をクリックしたときこのアクションを取得する。リンク制御部１８のアドレス生成部２０はユーザ端末１２のブラウザに設定すべきアドレス、すなわち協力会社サイト３０のＵＲＬを生成する。通常、そのＵＲＬは固定であるが、ここでは後述のようにそのユーザの認証情報をＵＲＬに付加したうえでブラウザへ設定する。ブラウザはＵＲＬに付加された認証情報を抽出し、本来のＵＲＬ部分のみを協力会社サイト３０へのアクセスへ利用するとともに、協力会社サイト３０からユーザＩＤとパスワードの入力が求められたとき、前述の抽出した認証情報を協力会社サイト３０へ自動的に送信する。この機能は最近標準的に利用されるウェブブラウザに実装される機能であり、本実施の形態ではそれを利用する。以上の処理の結果、ユーザのアクセス先は概念的に図中の経路ｔを辿り、ユーザ端末１２の接続先が図中の経路ｕにしたがって協力会社サイト３０となる。

【００２６】期限設定部２２は、ユーザが協力会社サイト３０にアクセスできる有効期限を設定する。期限設定部２２は協力会社サイト３０の図示しない認証サーバに後述の「アクセス許可ユーザリスト」をＦＴＰ（File Transfer Protocol）で送信する。そのリストには、協力会社サイト３０へのアクセスを認めるユーザの認証情報が記述されており、協力会社サイト３０の認証サーバは、そのリストを見てユーザのアクセスを制限する。

【００２７】図２はユーザがリンクを辿る際に生成されるＵＲＬを示す。まず、ユーザは最初に認証情報であるＩＤとパスワード（図中ＩＤ：ＰＷ）を入力して会員管理サイト１４へのログインを試みる。認証部１６は認証情報を取得してログインを認めるとともに、この情報をアドレス生成部２０へ通知する。アドレス生成部２０は認証情報を付加してＵＲＬを以下のように生成し、これがユーザ端末１２のブラウザに設定される。

http://ID:PW@www.web-b.com/xxx

【００２８】図３は前述のアクセス許可ユーザリスト３２を示す。アクセス許可ユーザリスト３２には協力会社サイト３０へのアクセスを認めるユーザの認証情報がログインした順のシリアル番号によって記述されている。ここでは、ログイン番号３３～５０のユーザ、つまり認証情報として「ＩＤ３３：ＰＷ３３」～「ＩＤ５０：ＰＷ５０」のユーザのアクセスが許可されている。アクセス許可ユーザリスト３２は期限設定部２２から協力会社サイト３０へ例えば１時間に１回送信され、次回送信の際、現在リストアップされている認証情報がクリアされ、「ＩＤ５１：ＰＷ５１」以降の認証情報が代わりに記述される。この方法により、ユーザのアクセスを１時間に限ることができる。なお、ここでは「アクセスを認めるための有効期限」といったが、これはログインできる有効期限やセッションの継続時間としての有効期限を含む。セッションの継続時間が１時間を超えたとき、協力会社サイト３０の認証サーバその他の構成はその旨をユーザへ通知して再ログインを促してもよい。

【００２９】図４は以上の構成によるサービスの一例を示す。会員用画面４０は、ユーザが最初に会員管理サイト１４の認証を受けてログインしたときに現れる。ここでは、会員管理サイト１４によるサービスが「○○○オンラインモール」と表示され、このユーザが「会員△△△」と表され、会員には割引の特典がある旨が示されている。画面下部には「商品ディレクトリ」のタイトルのもと、「日用品」「家具」「衣料品」などが列挙されている。ここでユーザが衣料品のリンク４２をクリックすると、リンク制御部１８でそのアクションが取得され、以降上述の処理を経て「衣料品」を担当する協力会社サイト３０へのアクセスが実現する。

【００３０】以上、本実施の形態によれば、ユーザは会員管理サイト１４へログインすれば協力会社サイト３０へのログインに際して再度認証手続を行う必要がない。

このため、ユーザの利便性が高まると同時に、会員管理サイト１４と協力会社サイト３０の連携によるサービスに一体感が出る。また、協力会社サイト３０も実際には会員管理サイト１４からの認証情報を用いた認証をしているため、セキュリティも配慮されている。さらに、アクセスに有効期限を設けたため、協力会社サイト３０のＵＲＬがブックマークされた場合でも、会員以外の者は容易にアクセスができない機構が実現する。

【００３１】なお、図２では理解の簡単のために、ユーザが入力した認証情報である「ＩＤ：ＰＷ」がそのままアドレス生成部２０によって生成されるＵＲＬに組み込まれる形で説明したが、現実には両者は異なることが、セキュリティ上もアドレス生成アルゴリズムの単純化の上でも望ましい。このために、アドレス生成部２０によって生成されるＵＲＬに組み込まれる「ＩＤ：ＰＷ」にワンタイム性をもたせればよく、一例として単純にシリアル番号を付与すればよい。その場合、図３のアクセス許可ユーザリスト３２の内容も単純にシリアル番号の記載で済み、管理上もリスト作成上もメリットがある。ただし、よりセキュリティを高める観点からいえば、当然ワンタイム化に際してランダマイズ等の処理を加えることが望ましい。

【００３２】実施の形態２．図５は実施の形態２に係るログイン管理システム１００の構成を示す。実施の形態１と異なり、代理サーバ１１０が設けられ、ユーザの協力会社サイト３０へのアクセスが代理サーバ１１０を通じて行われる。実施の形態２では、代理サーバ１１０を会員管理サイト１４と類似のドメイン名を利用して構築＊できる。

＊http://ztAjJ4kiq1SI.web-a.abc-proxy.com　（式１）

【００３５】ユーザは会員管理サイト１４にログインし（経路ｓ）、会員専用のページで協力会社サイト３０へのリンクを見つけ、これをクリックする。アドレス生成部２０はそのＵＲＬに有効期限を付加してブラウザへ設定する。これでユーザのアクセス先が代理サーバ１１０になる（経路ｕ）。代理サーバ１１０はＣＧＩ（Common Gateway Interface）などによりユーザからアクセスがあったとき、協力会社サイト３０から情報を取得してユーザへ転送するよう動作する。代理サーバ１１０はユーザに代わって協力会社サイト３０へログインし（経路ｖ）、協力会社サイト３０の情報をユーザへ閲覧させる（経路ｖ、ｗ）。これにより、実質的にアクセス先が会員管理サイト１４から協力会社サイト３０へ移動する（経路ｔ）。

【００３６】代理サーバ１１０は期限監視部１１２、認証要求部１１４、および情報転送部１１６を有する。認証要求部１１４は、ユーザがアクセスしてきたとき、協力会社サイト３０へログインするためにユーザＩＤとパスワードを送信して認証手続を要求する。このユーザＩＤとパスワードはユーザのものではなく、代理サーバ１１０自身のもので、協力会社サイト３０から代理サーバ１１０はひとりのユーザに見える。代理サーバ１１０が協力会社サイト３０へログインした後、情報転送部１１６は協力会社サイト３０の情報をユーザへ転送する。

【００３７】期限監視部１１２は、アドレス生成部２０がＵＲＬに埋め込んだ有効期限を検出して復号し、期限の到来を監視する。期限が到来したとき、代理サーバ１１０と協力会社サイト３０のセッションを切断する。

【００３８】図６は、ユーザが代理サーバ１１０へアクセスするまでの処理を示す。ユーザはまず、会員として最初に会員管理サイト１４へアクセスし、認証部１６による認証を受け（Ｓ１０）、会員管理サイト１４へログインする（Ｓ１２）。ユーザはつぎに協力会社サイト３０へのリンク個所をクリックする（Ｓ１４）。アドレス生成部２０は式１に示すＵＲＬを生成し（Ｓ１６）、これがユーザ端末１２のブラウザに設定され、代理サーバ１１０へのアクセスが実現する（Ｓ１８）。

【００３９】図７は代理サーバ１１０からユーザ端末１２に情報が提供される処理を示す。ユーザからアクセスされたとき、またはそれ以前の任意のタイミングにおいて、協力会社サイト３０は認証要求部１１４からのログイン要求に応じてこれを認証する（Ｓ３０）。認証後、

【００３３】ユーザから協力会社サイト３０へのリンクは、実施の形態１同様、会員管理サイト１４へログインできた会員のみから見え、また協力会社サイト３０へのアクセスが代理サーバ１１０で中継される。そのため協力会社サイト３０のセキュリティは高い。代理サーバ１１０はユーザの代わりに協力会社サイト３０の情報を取得するため、協力会社サイト３０から見ればひとりのユーザとして認証を受ける。いわゆる代理サーバが、その代理するサイトとの間でＩＤ、パスワードなどによる認証手続を経る点に特徴的である。以下、実施の形態１同様の構成には同じ符号を与え、実施の形態１との差を中心に説明する。

【００３４】期限設定部２２はアドレス生成部２０内部へ移動し、アドレス生成部２０はさらに暗号化部１０２を有する。この実施の形態では、暗号化部１０２で生成された有効期限は、暗号化部１０２で暗号化された後、ＵＲＬに付加される。ただし、そのＵＲＬは協力会社サイト３０ではなく代理サーバ１１０を指している。有効期限はリストに記述されるのではなく、アクセスの「開始時刻」と「終了時刻」などの形で直接的に記述される。ＤＮＳ（Domain Name Server）にはその標準的な機能としてワイルドカード指定が可能なものがあり、この実施の形態では、ワイルドカードの部分に有効期限を書き込む。アドレス生成部２０で生成されるＵＲＬの一例は以下のとおりであり、この暗号化された「ztAjJ4kiq1SI」の部分をワイルドカード指定してＤＮＳを通す。

代理サーバ１１０は協力会社サイト３０へログインする（Ｓ３２）。ユーザが代理サーバ１１０へアクセスしたとき、そのユーザに関する有効期限が到来していなければ（Ｓ３４のＮ）、情報転送部１１６がユーザのアクションを取得して（Ｓ３６）必要なページを協力会社サイト３０からユーザ端末１２へ転送する（Ｓ３８）。この後、有効期限が到来するまで同様の処理を繰り返し、期限が来たら（Ｓ３４のＹ）、そのユーザのためのセッションを切断し（Ｓ４０）、処理を抜ける。

【００４０】以上、本実施の形態によれば、ユーザが仮に協力会社サイト３０をブックマークしようとしても代理サーバ１１０のＵＲＬしかわからず、そのＵＲＬも有効期限で無意味になるので、会員でないユーザがこのユーザ端末１２を利用しても協力会社サイト３０の情報が得られない。有効期限は暗号化されているため、これをもとに有効期限を操作することもきわめて困難である。有効期限を開始時刻や終了時刻のように刻々変化する情報で表現するため、暗号化された情報のワンタイム性も高く、さらにセキュアである。

【００４１】以上、本発明を実施の形態をもとに説明した。この実施の形態は例示であり、それらの各構成要素や各処理プロセスの組合せにいろいろな変形例が可能なこと、またそうした変形例も本発明の範囲にあることは当業者に理解されるところである。

【００４２】例えば、図４では電子モールを例示した。しかし、本発明はそれ以外にも種々のサービスに利用可能である。一例として協力会社サイト３０に機密性のある情報を配し、会員管理サイト１４で閲覧者を管理する。例えば、協力会社サイト３０が製薬会社の場合、劇薬その他のデータの閲覧に医師の資格が必要である。協力会社サイト３０として複数の製薬会社を接続し、それ＊

＊らが機密情報を含む各種情報を医師に提供する場合、会員管理サイト１４はアクセスしてきたユーザが医師であるかどうかを確認した後、サービスを提供する。

【００４３】

【発明の効果】本発明によればログインに際してユーザの利便性が高まる。または、本発明によればサービスの一体感が高まる。

【図面の簡単な説明】

【図１】　実施の形態１に係るログイン管理システムの構成図である。

【図２】　実施の形態１において、アドレスが生成される様子を示す図である。

【図３】　実施の形態１で利用されるアクセス許可リストの構成図である。

【図４】　実施の形態１の会員管理サイトにアクセスしたときに表示される画面を示す図である。

【図５】　実施の形態２に係るログイン管理システムの構成図である。

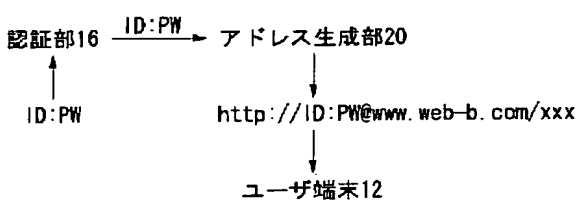
【図６】　実施の形態２において、アクセス先が代理サーバへ移行するまでの処理を示すフローチャートである。

【図７】　実施の形態２において、代理サーバからユーザ端末へ情報が提供される処理を示すフローチャートである。

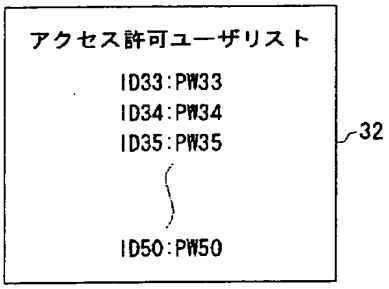
【符号の説明】

１０，１００　ログイン管理システム、　１２　ユーザ端末、　１４　会員管理サイト、　１６　認証部、　１８　リンク制御部、　２０　アドレス生成部、２２　期限設定部、　３０　協力会社サイト、　１０２　暗号化部、　１１０代理サーバ、　１１２　期限監視部、　１１６　情報転送部。

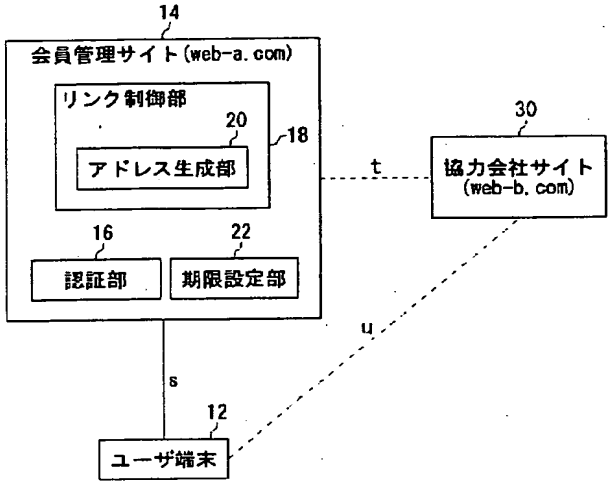
【図２】



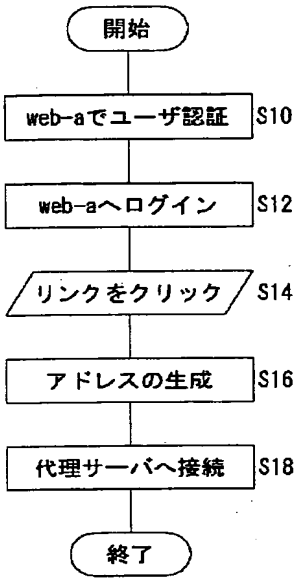
【図３】



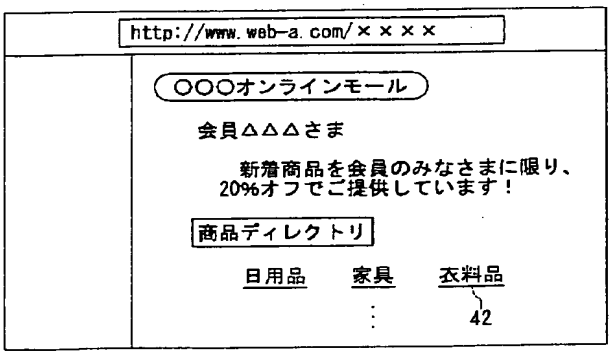
【図１】


14
会員管理サイト(web-a.com)
リンク制御部
20
18
アドレス生成部
30
協力会社サイト
(web-b.com)
t
16
22
認証部
期限設定部
u
s
12
ユーザ端末
10

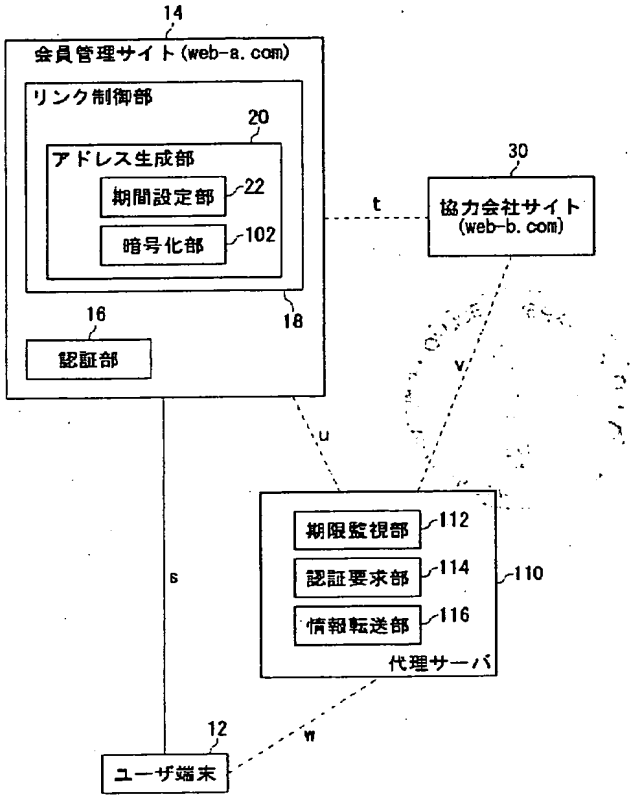
【図６】


開始
web-aでユーザ認証
S10
web-aへログイン
S12
リンクをクリック
S14
アドレスの生成
S16
代理サーバへ接続
S18
終了

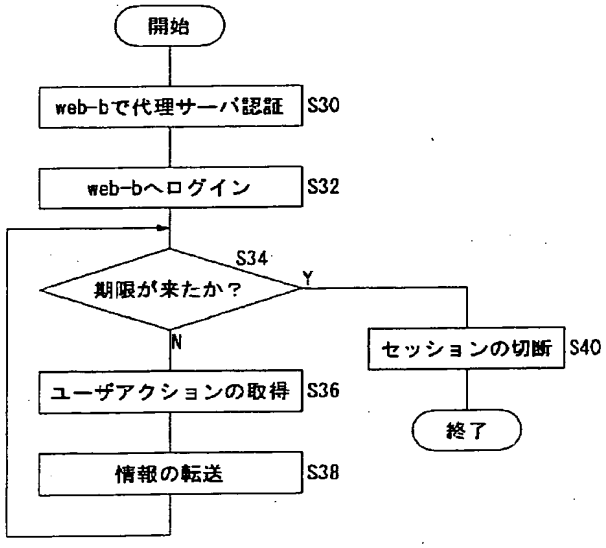
【図４】


http://www.web-a.com/××××
○○○オンラインモール
会員△△△さま
新着商品を会員のみなさまに限り、
20%オフでご提供しています！
商品ディレクトリ
日用品
家具
衣料品
42
40

【図５】


14
会員管理サイト(web-a.com)
リンク制御部
20
アドレス生成部
期間設定部
22
暗号化部
102
18
16
認証部
30
協力会社サイト
(web-b.com)
t
u
v
s
期限監視部
112
認証要求部
114
情報転送部
116
110
代理サーバ
12
w
ユーザ端末
100

【図７】


開始
web-bで代理サーバ認証
S30
web-bへログイン
S32
S34
期限が来たか？
Y
N
セッションの切断
S40
ユーザアクションの取得
S36
終了
情報の転送
S38